

Governor's Notice of Disapproval
LSA Document #20-366

December 10, 2020

Curtis T. Hill, Jr.
Indiana Attorney General
Indiana Government Center South, Fifth Floor
302 West Washington Street
Indianapolis, Indiana 46204-2770

RE: *Data Privacy – Security Breaches Rule, LSA 20-366(F)*

Dear General Hill:

I write in response to your proposed Indiana Administrative Rule governing data security breaches, LSA 20-366(F), which was submitted to me for review in accordance with the normal rulemaking process. Given the importance and potential impact of the proposed rule, I requested additional time for my review and consideration. While I appreciate all of the work you and your office have done in an attempt to provide clarity to businesses regarding their obligation to protect personal information, I have a number of concerns with the proposed rule as written and, for the reasons stated below, am hereby denying its approval.

Let me begin by acknowledging the merits of what the proposed rule seeks to accomplish. Protection of the personal information of Hoosiers is of paramount importance. I know many "data base owners" (Hoosier businesses and other businesses servicing Hoosiers) go to great lengths to protect the personal information of their customers, clients and employees from cyber criminals who seek to exploit the information to commit fraud, identity theft and other crimes. Many in the business community also know data breaches may well lead to a loss of customer trust as well as administrative and other legal actions. It is in everyone's best interest for data base owners to have strong measures in place to protect personal information. It is also vitally important that businesses have clear and reasonable rules and regulations so they know what is expected of them.

It is without question the goal of providing clarity to the business community is not only laudatory but needed. I find, however, the proposed rule does not provide the business community with sufficient clarity and further, in some instances conflicts with other protection and reporting obligations placed on certain businesses by the Indiana General Assembly. With my denial, I am also asking the Indiana General Assembly to review currently enacted data security laws for possible revision or enhancement to ensure Hoosier personal information is protected.

The Indiana General Assembly recognized the importance of protecting Hoosiers and providing direction to the business community when it enacted [IC 24-4.9](#) and required businesses to notify affected Indiana residents, your office, and in certain circumstances, credit reporting agencies, when a security breach of personal information occurs. [IC 24-4.9-3-3.5\(c\)](#) provides:

A data base owner shall implement and maintain reasonable procedures, including taking any corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner.

I find your proposed rule appropriately seeks to define and delineate "reasonable procedures" by listing a series of steps which businesses should take. And your proposed rule also establishes legal protection, also known as a "safe harbor" for businesses who follow the recommended steps. I commend you for outlining the steps businesses could and should take to reasonably protect personal information. Businesses which follow reasonable procedures should be afforded a safe harbor as you provide in the proposed rule.

Your proposed rule also delineates the minimum steps needed to be taken to be considered "appropriate corrective action" required by the statute. Again, I find your proposed rule appropriately outlines reasonable steps businesses should take when a data breach occurs. However, in the proposed rule, you have additionally afforded your office the authority to "conduct random and unannounced audits" of a data base owner without any limitation as to the scope or duration of such audits. While the use of audits is appropriate and can certainly assist in achieving compliance, the unlimited nature of this authority is problematic. As you know from comments made

publicly with regard to this rule, this provision without limitations has created a significant concern in the business community. I concur with their concerns.

Another provision in the proposed rule also raises concerns. The proposed rule makes it a deceptive act to fail to "implement and maintain a written data security plan that is reasonably designed to prevent a breach of security of data." Many have noted, and I concur, this provision essentially establishes strict liability on business owners. This provision goes beyond defining what would prevent a business owner from claiming safe harbor status and instead expands the acts and actions which constitute "deceptive acts" under the statute. I believe this is the province of the Indiana General Assembly.

Yet another area of concern is the failure to exempt the insurance industry from the proposed rule given the Indiana General Assembly, just last session, enacted [IC 27-2-27](#) which sets out comprehensive data security requirements and standards for that industry. More importantly, the law gives exclusive authority to the Indiana Department of Insurance to regulate data security for their licensees, which would include insurance companies, agents, and most other entities associated with the industry. Your proposed rule cites to [IC 27-2-27](#) as an acceptable standard for a business to adopt. It follows that your rule seeks to oversee and regulate the insurance industry contrary to Indiana law.

As I stated at the beginning, I fully support the concept of the rule; however, I believe the rule can be improved. Pursuant to [IC 4-22-2-34](#), I am therefore disapproving this rule and returning it to you.

Sincerely,

Eric J. Holcomb
Governor of Indiana

Posted: 12/16/2020 by Legislative Services Agency
An [html](#) version of this document.